UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

DAVID HOUSE, Plaintiff, v. JANET NAPOLITANO, in her official capacity as Secretary of the U.S. Department of Homeland Security; ALAN BERSIN, in his official capacity as Commissioner, U.S. Customs and Border Protection; JOHN T. MORTON, in his official capacity as Director, U.S. Immigration and Customs Enforcement, Defendants.	)	Case No. 1:11-cv-10852-DJC (Leave to file granted 10/28/2011)

DEFENDANTS' REPLY TO PLAINTIFF'S OPPOSITION TO THEIR MOTIONTO DISMISS, OR IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES **PAGE(S)**

FEDERAL RULES

After two-hundred plus years of routine Government searches of items passing into and out of the United States, Plaintiff asserts that electronic devices are so unusual and so different that they require an entirely new rule than what has regularly applied at the border. Plaintiff so asserts despite the fact that electronic devices are, in fact, nothing more than a means to store information, just as suitcases can store items. Indeed, the Supreme Court has permitted searches of containers similar to Plaintiff's devices (and the information stored therein) at the border since the founding of our nation, including contents such as books, magazines, papers, microfiche, and film canisters. Such containers and their contents may contain personal and intimate information, but courts hearing similar claims regarding border searches of electronic devices have rejected them. Nothing in Plaintiff's papers make a persuasive case for this Court to adopt an exception to the Government's border search authority for electronic devices. Nor is there a basis for the Court to impose hard and fast limits on how long the Government may take to search such devices, when it can explain the reasons for the duration of a search, as it has done in this case. Finally, while Plaintiff makes allegations about the Government's efforts to target him and the group with which he claims association, the Complaint lacks supporting details that would render his allegations plausible. As such, his Complaint fails to state a claim upon which relief can be granted, and it should be dismissed.

I. PLAINTIFF HAS FAILED TO STATE A FOURTH AMENDMENT CLAIM

Plaintiff breaks his argument into three parts, but they are all based on one premise — that electronic devices require special treatment at the border because they can store large amounts of personal information. Opp. at 11-19. But as federal appellate courts have uniformly held, electronic devices are not so unlike any other item that has ever crossed the border such that the Government's border search authority should be constrained as Plaintiff suggests.

A. The Search of Plaintiff's Electronic Devices Was a Routine Border Search

In his effort to argue for a special exception for electronic devices at the border, Plaintiff presents the same arguments that have been rejected by every federal appeals court to consider the issue. Analogizing electronic devices to closed containers, like suitcases, is not Defendants' invention; instead, that analogy has been consistently and recently affirmed by the Ninth and Fourth Circuits as well as a variety of district courts, including two in the First Circuit. *See* Defs. Br. at 10-16. Plaintiff is thus left to rely on dissenting opinions (Opp. at 10); cases that are more than 35 years old (Opp. at 19 and n.8, 20); and cases involving domestic searches and search warrants, circumstances where traveler expectations and Government interests are very different (Opp. at 13, 14, 17, 18, 20).

For instance, Plaintiff's comparison of electronic devices to homes (Opp. at 14) is misguided. A computer is not a home; it is a device that can store information. Likewise, arguing that Government's position equates the search of a laptop with a search of "socks" and "contact lens solution" (Opp. at 10) is also erroneous. The appropriate comparison is a search of Plaintiff's devices with a search of suitcases filled with microfiche, paper, books, or films. Ultimately, electronic devices are a means of storage, just as is luggage, and the Government's border search authority over closed containers and the items therein is already well established. *See* Defs. Br. at 10-16.[1]

[1] Even the border search cases that Plaintiff does cite are distinguishable. *See United States v. Laich*, No. 08-20089, 2010 WL 259041, at *2 (E.D. Mich. Jan. 20, 2010) (Laich had proceeded to his connecting flight and had to be "escorted back to the customs inspection area" before his laptop and camera were detained by CBP); *United States v. Yang*, 286 F.3d 940, 947 (7th Cir. 2002) (Teng was detained "at a completely different airport terminal" after he had left the international terminal); *United States v. Stewart*, 715 F. Supp. 2d 750, 754-55 (E.D. Mich. 2010) (court opinion relied on the now-reversed *Cotterman* district court opinion). Here, Plaintiff was still in the federal inspection service area, which meant that he maintained his nexus to the border during the search. *See* Harris Decl., ¶¶ 4-8; Louck Decl., ¶¶ 5-9; Santiago Decl., ¶¶ 5-9. As a result, there is no colorable claim that the secondary inspection of Plaintiff was an extended border search.

Plaintiff contends that searches of electronic devices warrant a special rule because they are non-routine, particularly offensive, and impose a serious burden on First Amendment activity. Opp. at 11-19. By continuing to press for a special rule for electronic devices because of how they are used, Plaintiff is asking this Court to engage in the kind of line-drawing that the Supreme Court has already rejected. In *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004), the Supreme Court reversed a decision where the circuit court had "fashioned a new balancing test [for border] searches of vehicles." The Supreme Court held that using special "tests to determine what is a 'routine' search of a vehicle, as opposed to a more 'intrusive' search of a person, have no place in border searches of vehicles." *Id.* In this vein, the *Braks* case Plaintiff repeatedly cites is also of questionable value, since it too had fashioned a multi-factor test to determine if a border search is routine. *United States v. Braks*, 842 F.2d 509, 514 (1st Cir. 1988). *See United States v. Arnold*, 533 F.3d 1003, 1008 (9th Cir. 2008) (stating that "*Flores-Montano* rejected our prior approach of using an intrusiveness analysis to determine the reasonableness of property searches at the international border").[2]

The search of electronic devices is not a "personally invasive" search; indeed, this category of searches has *only* been extended to searches of the body such "strip searches and body cavity searches." *United States v. Amaro-Rodriguez*, No. 08-378, 2010 WL 503063, at *2

[2] The district court in *Flores-Montano* relied on *United States v. Molina-Tarazon*, 279 F.3d 709 (9th Cir. 2002), to find that the search of the vehicle was unlawful. In *Molina-Tarazon*, 279 F.3d at 713, the court listed three factors to conclude that the relevant search violated the Fourth Amendment: "Force was used to remove and disassemble the fuel tank; the procedure involved some risk of harm; and someone whose vehicle was subjected to such a search is likely to feel a diminished sense of security." The *Molina-Tarazon* court went on to say that these three factors might not be all that was relevant; indeed, it noted "[t]hese happen to be the factors relevant in our case. We do not rule out the possibility that other factors, such as protracted delay in completing the search, may render a search nonroutine." *Id.* at 713 n.5. This kind of indistinct, multi-factor analysis makes the line between routine and non-routine border searches very difficult to draw, as the Supreme Court acknowledged.

(D.P.R. Feb. 8, 2010); *United States v. Barrow*, 448 F.3d 37, 41 (1st Cir. 2006).[3] Indeed, for searches of property, the relevant question is whether the search was conducted in a "particularly offensive manner" or resulted in excessive damage. *See Flores-Montano*, 541 U.S. at 154 n.2 (quoting *Ramsey*, 431 U.S. at 618 n.13); *United States v. Chaudhry*, 424 F.3d 1051, 1054 (9th Cir. 2005) (rejecting, as a result of *Flores-Montano*, a distinction between "routine" and "nonroutine" searches of property). There are no allegations in the complaint that Plaintiff's devices were harmed in any way or that the search was conducted in a "particularly offensive manner."

B. Electronic Devices Do Not Deserve a Special Carve-Out from the Government's Long-Standing Border Search Authority.

There is nothing inherently expressive about electronic devices; instead, they are merely an electronic means of storage. As such, they are no different than a suitcase full of books and papers. Plaintiff's contention that the "revolutionary" and "participatory" nature of electronic devices (Opp. at 15) means that they cannot be compared with a suitcase ignores the fact that the Government's search of the devices occurs at a fixed point in time, *i.e.*, when the devices are coming into or out of the country.[4] The same is true for suitcases; suitcases may contain different items just days after a border search, but the search ensures the Government is able to search items brought by travelers across the border.

While Plaintiff contends his expressive interests have been chilled by the search of his devices, any such effect is an incidental result of a valid border search. Moreover, such arguments are hardly new, as travelers have previously made the same arguments about the

[3] In his declaration, Plaintiff states that the detention took about an hour (House Decl., ¶ 11), which is well within the amount of time the Government may detain individuals for questioning at the border. *See Flores-Montano*, 541 U.S. at 155 n.3 ("We think it clear that delays of one to two hours at international borders are to be expected.").

[4] Plaintiff's devices were never cleared for entry into the United States. Instead, the devices were detained so that customs officials could complete their border search of the devices. *See* Marten Decl., ¶¶ 5-6.

expressive content of border searches of films, books, and documents. *See Church of Scientology of Cal. v. Simon*, 460 F. Supp. 56, 57-58 (C.D. Cal. 1978) (three-judge panel rejected plaintiff's constitutional challenge to border search of "thousands" of Church of Scientology papers; neither the authorizing statute or the method of enforcement presented constitutional problems); *United States v. 12 200-Ft. Reels of Super 8mm. Film*, 413 U.S. 123, 125 (1973) (rejecting constitutional challenge to border search seizing obscene "movie films, color slides, photographs, and other printed and graphic materials" even where owner contended the items were for his personal use); *United States v. Seljan*, 547 F.3d 993, 1003 (9th Cir. 2008) (*en banc*) (rejecting constitutional challenge to border search of "an envelope containing personal correspondence"), *cert. denied*, 129 S. Ct. 1368 (2009). These same arguments have been rejected more recently by several courts in the context of electronic devices specifically. *See Arnold*, 533 F.3d at 1010; *United States v. Ickes*, 393 F.3d 501, 507 (4th Cir. 2005).

Furthermore, the very reasons Plaintiff says that his electronic devices are special and thus deserving of an exception to the well-established border search rule highlight why the devices should be subject to routine searches at the border. As Plaintiff himself notes, the devices can store large amounts of data, ranging from photographs and documents to websites and e-mails. Opp. at 13. He reasons that the more information a device may contain, the less authority the Government has to search it. But, in fact, the more information a device may hold, the more the Government's interest in securing its borders is served by such a search. At the border, travelers carrying electronic devices are attempting to bring them into or out of the United States, and the Government has a right to know what is coming in or going out of the country. A carve-out for electronic devices from routine border search authority could "create a sanctuary at the border for all expressive material—even [ ] terrorist plans . . . [and] would

undermine the compelling reasons that lie at the very heart of the border search doctrine." *Ickes*, 393 F.3d at 506; *see also United States v. Irving*, No. 03-cr-633, 2003 WL 22127913, at *5 (S.D.N.Y. Sept. 15, 2003) ("any other decision effectively would allow individuals to render graphic contraband, such as child pornography, largely immune to border search simply by scanning images onto a computer disk before arriving at the border."). Indeed, the Government recently arrested a man on charges of planning to use small, explosive-laden drones to attack the Pentagon and the Capitol; he stored information about the plot on two flash drives, including numerous pictures as well as a detailed plan, featuring sections entitled "Hardware and Aircraft configuration" and "Software Overview." *See* Peter Finn, "Mass. man accused of plotting to hit Pentagon and Capitol with drone aircraft," Wash. Post (Sept. 28, 2011), http://www.washingtonpost.com/national/national-security/mass-man-accused-of-plotting-to-hit-pentagon-and-capitol-with-drone-aircraft/2011/09/28/gIQAWdpk5K_print.html. Thus, the Government's ability to routinely search electronic devices at the border helps protect and defend the nation.

C. Plaintiff's Allegations About the Government's Subjective Motivations for the Search of his Devices Are Irrelevant to his Fourth Amendment Claim

Plaintiff alleges that he was singled out for a search, but allegations about an officer's subjective motives for a border search, even assuming they are true, are irrelevant to a Fourth Amendment analysis. *See, e.g., Whren v. United States*, 517 U.S. 806, 813 (1996) (stating that "we have been unwilling to entertain Fourth Amendment challenges based on the actual motivations of individual officers"). Instead, "the level of intrusion into a person's privacy is what determines whether a border search is routine." *United States v. Irving*, 452 F.3d 110, 123 (2d Cir. 2006). As explained above, because electronic devices are another type of closed

containers, the Government has a right to routinely search such devices coming into or out of the United States by travelers without suspicion.

D. Plaintiff's Devices Were Detained for a Reasonable Period of Time

There is no hard and fast rule for how long the Government may detain items that it has *not* finished searching when they are detained at the border. Plaintiff's opposition shows that he regards the routine search of any electronic device, at any time, for any length of time, as unlawful. Indeed, the very allegations Plaintiff makes about the volume of information contained on his devices show precisely why the devices cannot be searched quickly, and why such searches may need to occur away from the initial border checkpoint. Even Plaintiff admits that such searches require specific kinds of software and equipment. *See* Stamos Decl., ¶¶ 10-14.

The Fourth Amendment "contains no requirements about *when* the search or seizure is to occur or the *duration*." *United States v. Gerber*, 994 F.2d 1556, 1559 (11th Cir. 1993) (emphasis in original). Courts have recognized the unique nature of computer searches, the computer's enormous data storage capacity, and the inherent delay involved in conducting a comprehensive forensic analysis of computer records. *See, e.g., United States v. Hernandez*, 183 F. Supp. 2d 468, 480 (D.P.R. 2002) (neither Fed. R. Crim. P. 41 nor the Fourth Amendment "provides for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant," and where delay occurs "extensions or additional warrants are not required."); *United States v. Triumph Capital Grp., Inc.*, 211 F.R.D. 31, 66 (D. Conn. 2002) (noting that "computer searches are not, and cannot be subject to any rigid time limit because they may involve much more information than an ordinary document search").

E. No Genuine Disputes of Material Facts Preclude the Entry of Summary Judgment

Defendants' declarations establish that the detention of Plaintiff's devices was

reasonable. Special Agent Marten's declaration explains the basis for his statements; that he received Plaintiff's devices when they were sent to his office, and that he was personally involved in the effort to image Plaintiff's devices after they were detained on November 3, 2010. Marten Dec., ¶¶ 5-14. His eight-year background as an ICE agent provides a basis for him to explain the responsibilities and obligations of ICE agents staffed on computer forensic assignments. *Id.*, ¶¶ 1, 13. Plaintiff contends that he needs discovery to fill the "many holes" in Defendants' submissions; he wants to know whether the ICE agents at O'Hare had prior knowledge of Plaintiff or the Support Network (Opp. at 4 n.2) – but such information is not relevant to a Fourth Amendment analysis. *See* supra at I.C. Plaintiff also wants information about any ICE backlog, and a breakdown of which factors described in Agent Marten's Declaration account for which days Plaintiff's devices were detained (assuming such an accounting could even been prepared). Opp. at 23. Such information is not required, as Defendants' submissions show that ICE reasonably processed Plaintiff's devices, and there is no need for the Court to permit any discovery on these issues. *See* Fed. R. Civ. P. 56(a).

In his opposition, Plaintiff submitted the unsworn declaration of Alexander Stamos, an employee of a private sector company, iSec Partners.[5] Mr. Stamos has no experience working for the Government or any connection to law enforcement, and his essential point is that, in the private sector, the imaging of Plaintiff's devices could have taken less time. This point is neither novel nor relevant.

Unlike ICE, which is primarily a law enforcement agency, Mr. Stamos's firm is "a full-service application, infrastructure and mobile security consulting company combining cutting edge research with an unflagging commitment to customer service." *See* iSec Partners,

[5] The Stamos declaration was not signed under penalty of perjury so it should not be considered under Rule 56(c)(4). *See Bourne v. Town of Madison*, 494 F. Supp. 2d 80, 91 n.5 (D.N.H. 2007). But to ensure that these issues are fully vetted for this Court, however, Defendants have undertaken to respond to its substance.

http://www.isecpartners.com/ (last visited Oct. 26, 2011). There are 220 ICE agents trained in computer forensics who "respond to border searches" at all 327 ports of entry; ICE's responsibilities include " deterring, interdicting, and investigation threats arising from the movement of people and goods into and out of the United States" through civil and criminal laws. Marten Decl., ¶¶ 2, 13. In contrast, Mr. Stamos's firm provides "information security consulting" services for various private sector companies. Stamos Decl. ¶ 2.[6] There is no reason for this Court to find Mr. Stamos's declaration relevant, since it says nothing about how ICE functions, given ICE's many responsibilities, of which searches of electronic devices are only part.

In addition, private sector companies may not be required to meet chain-of-custody requirements, as is required in a law enforcement context when electronic devices are searched. *See United States v. McNealy*, 625 F.3d 858, 867 (5th Cir. 2010) ("The forensic imaging process produced an exact copy of the digital files on McNealy's computer, these files were then captured on DVDs, and the exhibits were printed from the DVDs. The Government presented evidence establishing the chain of custody and the technology utilized."); *Sweeney v. DHS*, 233 Fed. Appx. 997, 999 (Ct. Fed. Cl. 2007) (upholding 30-day suspension of ICE agent who failed to "follow specific procedures designed to protect the chain of custody of evidence").

Mr. Stamos has never worked at ICE; indeed, his resume does not indicate any work on behalf of the Government. Stamos Decl. at p. 26-27. Moreover, much of his affidavit reflects disagreements Mr. Stamos appears to have about how ICE agents work – he contends that certain

[6] Moreover, other litigation in which Mr. Stamos has been involved reveals that there may be little agreement over the best way to generate forensic copies. *See Berlage v. Google*, No. 10-02817, Dkt. # 9 (N.D. Cal.), Pl's. Ex Parte Mot. for Temp. Rest. Order and Prelim. Injunc. at 11 and 16 (filed June 3, 2010) (Plaintiff contended that "the techniques employed by Google's expert, Mr. Stamos, fail to describe a process that would ensure that data is preserved" and although "Mr. Stamos purports to have taken steps that would appear to a lay person to have secured data, he in fact took steps that would ensure that data tampering and deletion could not be detected by computer forensic imaging.").

technology (Linux, as well as dual configurations for laptops) is standard, while in ICE's experience, it is non-standard. Stamos Decl., ¶ 21; Marten Dec., ¶ 11. Mr. Stamos thinks the set-up of Plaintiff's devices is common; in ICE's experiences, such a set-up is not. Marten Dec., ¶ 11. Mr. Stamos's personal opinions about what he believes to be standard fail to create a *genuine* dispute of a *material* fact because it sheds no light on the question before the Court, *viz.*, the reasons for the length of the detention of Plaintiff's devices by ICE.

II. PLAINTIFF HAS NOT MADE OUT AN ASSOCIATIONAL PRIVACY CLAIM

Plaintiff has not presented sufficient allegations for an associational privacy claim. There is no such violation just because the Government is retaining a copy of the information contained on his devices; the items were lawfully detained and searched; and the copies would already have been destroyed by ICE but for the litigation hold in place in connection to this litigation. Moreover, despite the time that has elapsed since the search and detention of his devices, the Complaint (and Plaintiff's declaration) lack any allegations that the Support Network has, in actuality, suffered in any way. All that has been presented are Plaintiff's personal predictions of what he expects will happen to the Support Network. For Plaintiff to plausibly make out this claim, allegations of more concrete and plausible harm to the Support Network are required.

A. The Search of Plaintiff's Expressive Material was Incidental to a Valid Border Search

Upon his re-entry to the United States, Customs officers referred Plaintiff for secondary inspection; this inspection included a thorough search of all the items he was carrying (including his laptop, a cell phone, a digital camera, and flash drive). Plaintiff contends the search was aimed at disrupting his "associational activity." Opp. at 25. None of the cases cited by Plaintiff involve information obtained as a result of the Government's border search authority (or as result of a similarly extensive source of government authority). Several cases cited by Plaintiff feature

subpoenas by government or other entities seeking specific information from an individual or entity.[7] Still others implicate domestic laws requiring disclosure of various affiliations or other information.[8] As a result, there was little need for such challengers to "extensively support" their claimed harm since the very provisions at issue compelled disclosures of specific information.

But in this case, any Support Network information was part of the Government's November 3, 2010 search because Plaintiff chose to bring such information with him when he traveled, stored on a device he presented for entry, at a U.S. border. This is not, therefore, a typical associational privacy case, where one party seeks specified information directly from the other via subpoena, discovery request, or statutory disclosure. Had Plaintiff chosen not to bring any Support Network materials with him when he traveled in November 2010, there would have been no such materials for the Government to search.

---

[7] *See Amazon.com LLC v. Lay*, No. C10- 664, 2010 WL 4262266, at *10-12 (W.D. Wash. Oct. 25, 2010) (civil subpoenas sought disclosure of customers' identities and purchases from Amazon to Washington State Department of Revenue); *In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461 et seq.*, 706 F. Supp. 2d 11, 12 n.1 (D.D.C. 2009) (grand jury subpoenas sought, among other items, "a copy of records that show the identity of all movies sold or distributed, including the date of each transaction, payment received, and method and date of each of each shipment, from customer purchases from the website/domain name www. [_____]. com between December 1, 2007 and December 15, 2007, and April 1, 2008 and April 15, 2008"); *Pollard v. Roberts*, 283 F. Supp. 248, 258 (E.D. Ark. 1968) (state prosecutor's subpoena sought information reflecting political party affiliations and campaign contributions); *In re Grand Jury Subpoena to Amazon.com*, 246 F.R.D. 570, 571-72 (W.D. Wis. 2007) (grand jury subpoena directed Amazon to "provide virtually all of its records regarding [grand jury target Robert] D'Angelo, including the identities of the thousands of customers who had bought used books from D'Angelo . . . grand jury is investigating whether D'Angelo evaded taxes or engaged in a mail fraud/wire fraud scheme involving [his] sale of about 24,000 used books over four years through Amazon's website to third-party book buyers."); *In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.*, No. 98-MC-138, 26 Med. L. Rptr. 1599, 1600 (D.D.C. Apr. 6, 1998) (subpoena issued by Independent Counsel sought all "documents and things referring or relating to any purchase by Monica Lewinsky").

[8] *See Shelton v. Tucker*, 364 U.S. 479, 480 (1960) (involving challenge to "Arkansas statute [that] compels every teacher, as a condition of employment in a state-supported school or college, to file annually an affidavit listing without limitation every organization to which he has belonged or regularly contributed within the preceding five years"); *Talley v. California*, 362 U.S. 60, 60-61 (1960) (involving challenge to Los Angeles city ordinance that banned the distribution of handbills "in any place under any circumstances" unless the handbill bore the name and address of the individuals "who printed, wrote, compiled or manufactured" the handbill as well as the name and address of the individual "who caused the same to be distributed"); *Johnson v. Washington Times Corp.*, 208 F.R.D. 16, 17-18 (D.D.C. 2002) (discovery request sought information related to religious affiliation of defendant's employees; court limited the scope of the subpoena, concluding that "plaintiff gives me no reason to doubt the word of Church officials and of a distinguished religious scholar (unaffiliated with the Church) that the Church is controversial and that its members have encountered bigotry and prejudice").

Moreover, Plaintiff's argument would mean that the Government would be required to show reasonable suspicion for any search of expressive materials (a result at odds with decades of caselaw), and for any materials which reflect involvement with any group that could conceivably be "controversial" or "highly charged." Certainly, that was not required by the three-judge panel that rejected a First Amendment challenge to the border search of "thousands of pages" of documents from the Church of Scientology (*Church of Scientology*, 460 F. Supp. at 57-58), an organization that has been the subject of controversy. *See* Federal Prosecutors Unveil the Astonishing Intrigues of the Scientology Church (Aug. 14, 1978), People Magazine, http://www.people.com/people/archive/article/0,,20071478,00.html.[9]

Nor do Plaintiff's alleged "watchlisting" allegations suffice to state an associational privacy claim. While Plaintiff alleges that he is a member of what he calls the "TECS II watchlist," a review of the relevant government authorities related to TECS establishes this is not the case. TECS is the database the Government uses to "provide a record of *any* inspections conducted at the border" and for which Defendants have issued a public System of Records Notice ("SORN"). *See* TECS SORN, (Dec. 19, 2008), http://edocket.access.gpo.gov/2008/E8-29807.htm (emphasis added). Individuals included in the TECS database include "[o]wners, operators and/or *passengers* of vehicles, vessels or aircraft traveling across U.S. borders or through other locations where CBP maintains an enforcement or operational presence" (emphasis added). As an international traveler, Plaintiff, therefore, is one of many individuals in

[9] Similarly, Plaintiff's argument could also mean that the Government would be subject to different legal standards for border searches depending on whether or not the individual involved is a member of a group or not. Individuals should not be exempt from routine border searches for such reasons. *Cf. Holderbaum v. United States*, 589 F. Supp. 107, 112 (D. Colo. 1984) ("an individual should not be insulated from tax liability or investigation into his tax liability merely because he is a member of a particular organization or deals with members of a particular organization."). Operationally, this limitation would make little sense in a border search context; the Government would presumably not be in a position to contradict a traveler's assertion of affiliation with a "controversial" group at the outset of the search, so it might be required to meet this higher standard for any (and all) travelers who so identified themselves.

the TECS system, and his inclusion therein indicates nothing unusual. The relevant Privacy Impact Assessment ("PIA") for TECS also notes that:

> CBP collects certain information from, and about, the traveling public at various stages of the international trip in order to perform law enforcement queries on the traveling public prior to and/or at the time of performing an inspection…
>
> For all individuals entering the U.S. at a POE, a record detailing the traveler's border crossing is captured through TECS…
>
> If the CBP officer at primary determines that additional inspection is needed, the traveler will be referred to secondary. A record of the referral and secondary inspection is entered into TECS as a Subject Record.

See http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf.[10] Here, any alleged infringement on Plaintiff's "right of association" was incidental to a valid exercise of the Government's authority to search and detain personal items at the border. Plaintiff is not free from searches at the border simply because he may be a member of a group.

B. Plaintiff Has Failed to Put Forward Any Allegations that Show the Support Network's Activities Have Been Curtailed by the Government's Search of his Electronic Devices

Defendants are not asking the Court to resolve "contested issues of fact" on his associational privacy claim. Opp. at 28. Instead, Plaintiff has not actually put any allegations that plausibly allege Government interference with the Support Network. Plaintiff, a Support Network Steering Committee member, offers no specifics on the alleged "chill" on the Support Network due to the 2010 search of his devices. Such facts are within Plaintiff's control. *See Brown v. Medtronic, Inc.*, 628 F.3d 451, 461 (8th Cir. 2010) ("a plaintiff is the master of his own

[10] Moreover, if Plaintiff has been questioned about Mr. Manning, such questioning can hardly be surprising, given that the Government is currently preparing a court-martial case against Mr. Manning, and Plaintiff has admitted that he formed an association with Mr. Manning before he was arrested. *See infra* at 14-15.

complaint" including its factual allegations). The absence of such allegations by Plaintiff is not a reason for this Court to deny the Government's motion.[11]

All that is presently before the Court are a series of inexact allegations about what Plaintiff thinks may happen to the Support Network and its members, none of which appears to have actually happened. Where almost a year has passed since the search at issue, Plaintiff must put forward more specific allegations to make out a plausible claim. The lack of such allegations fails to show the kind of specific "harassment and intimidation" required of parties claiming a First Amendment chilling effect. *In Re Motor Fuel Temperature Sales Practices Litig.*, 641 F.3d 470, 491 (10th Cir. 2011); *see also* Defs. Br. at 23-28.[12]

Plaintiff's allegations that he has been questioned about Mr. Manning, an individual against whom the United States is pursuing a criminal investigation, do not constitute a basis for a First Amendment claim. *See* House Compl., ¶ 14. Indeed, Plaintiff's admitted association with Mr. Manning thus forms an "obvious alternative explanation" for why he has been questioned by various Government agencies. *See Ashcroft v. Iqbal*, 556 U.S. 662, 129 S. Ct. 1937, 1951 (2009); *Bell Atl. v. Twombly*, 550 U.S. 544, 567 (2007). The Constitution does not forbid the Government from questioning individuals who may possess knowledge of violations

[11] Plaintiff's belated attempt to amend his complaint via his opposition (Opp. at 27 n.14) in an effort to bolster his deficient allegations is inappropriate and insufficient. Briefs are not a substitute for a proper motion to amend, and Plaintiff's after-the-fact allegation of the expression of "concerns" by alleged Support Network members still fails to state a claim for associational privacy. In addition, some of the cases Defendants cited do involve similar procedural circumstances to this case. *See In Re Motor Fuel Temperature Sales Practices Litig.*, 641 F.3d 470, 491 (10th Cir. 2011) (considering whether gas trade association, on a motion to compel made in response to initial discovery requests following the filing of a complaint, had made out a "prima facie case of privilege").

[12] The Second Circuit's opinion in *Tabbaa v. Chertoff*, 509 F.3d 89, 92 (2d Cir. 2007), does not support Plaintiff's First Amendment claim. Unlike Plaintiff's allegation of a single person being subjected to secondary screening, in *Tabbaa*, CBP instituted a special inspection operation pursuant to which all individuals who attended various conferences (specifically, certain Islamic conferences held during the year-end holiday season of 2004), who then sought entry into the United States "were subject to the kind of screening procedure normally reserved for suspected terrorists." 509 F.3d at 92. The five plaintiffs in *Tabbaa* had attended such a conference and were, consistent with the CBP operation, "detained by CBP officials for several hours, questioned, patted-down, fingerprinted, and photographed." *Id.* In addition, while the Second Circuit found that conference attendees did encounter "a direct and substantial interference with associational rights," the court nevertheless found that the government's actions did not violate their right of association. *Id.* at 101-103

of its laws. Courts have rejected such claims even when pressed by journalists. *See Branzburg v. Hayes*, 408 U.S. 665, 682, 692 (1972). It is equally plausible that Plaintiff has been questioned by Government officials because he is an admitted associate of a person suspected of serious criminal activity.[13] The Complaint, therefore, fails to set out a claim for associational privacy, since there are no plausible allegations of harm to the Support Network, and Plaintiff's individual allegations may also be related to his connections to a suspected criminal.

III. PLAINTIFF DOES NOT HAVE A CLAIM FOR IMPROPER DISSEMINATION AND RETENTION

Finally, there is no basis for this Court to deny summary judgment, or require discovery, because Plaintiff also claims that his information was improperly disseminated or retained. Under First Circuit precedent, any facts sought in discovery must "if obtained, . . . help defeat pending motion." *Vargas-Ruiz v. Golden Arch Dev., Inc.*, 368 F.3d 1, 4 (1st Cir. 2004). Plaintiff's allegations about improper dissemination and retention fail to state a claim for relief and do not bar the granting of Defendants' motion.

ICE detained the information in accordance with its statutory duties to search items coming into or out of the United States. *See* supra at I.A. Plaintiff identifies no source for a right to know what ICE did with the information it lawfully obtained. None of the associational

[13] Mr. Manning is currently facing an Army court-martial based on allegations that he "introduced unauthorized software onto government computers to extract classified information, unlawfully downloaded it, improperly stored it, and transmitted the classified data for public release and use by the enemy." *See* Army Adds 22 Charges Against Intelligence Analyst (Mar. 2, 2011), http://www.defense.gov/news/newsarticle.aspx?id=63002. Plaintiff has publicly written and spoken about his association with Mr. Manning, which was formed before Mr. Manning was arrested. *See* Michael Riley, "WikiLeaks Grand Jury Witness Says he Declined to Answer Queries on Manning" (June 15, 2011), http://www.bloomberg.com/news/2011-06-15/wikileaks-grand-jury-to-interview-computer-expert-friend-of-manning-today.html; *see* David House, "Bradley Manning Speaks About His Conditions" (Dec. 23, 2010) http://my firedoglake.com/blog/2010/12/23/bradley-manning-speaks-about-his-conditions (discussion of Plaintiff's visit to Mr. Manning in December 2010). Plaintiff admits he has been questioned about Mr. Manning and WikiLeaks (Opp. at 5); WikiLeaks is an organization which may be involved in "the stealing of and the dissemination of sensitive and classified information." White House Press Briefing (Nov. 29, 2010), http://www.whitehouse.gov/the-press-office/2010/11/29/press-briefing-press-secretary-robert-gibbs-11292010.

privacy cases Plaintiff cites involved a demand that the Government disclose how it had used any information that it had obtained. Opp. at 27-28.

There is also no limit on how broadly such a claim could reach. Any person whose personal possessions or information have been detained by ICE could demand that a court order ICE to disclose whether their information has been shared with other Government entities. Such disclosures could compromise the law enforcement functions ICE performs for the Government because it could inhibit (or interfere with) appropriate information sharing between agencies that would identify threats to the U.S.[14]

Nor is there a basis for Plaintiff to ask this Court to order ICE to destroy the information retained from the border search of Plaintiff's devices. ICE has already provided a declaration that indicated that the information would be destroyed but for the filing of this litigation. *See* Marten Dec., ¶ 15. And, assuming that the search of Plaintiff's electronic devices was unlawful, he still would not be able to obtain an order from the Court requiring destruction because there is nothing unlawful about the Government's retention of materials derived from a search later determined to be unconstitutional. *See, e.g., Illinois v. Krull*, 480 U.S. 340, 347-61 (1987). Accordingly, Plaintiff's requested relief does not state a legal claim for relief.

[14] Plaintiff contends that the Government has "admitted" the fact that it disseminated the information obtained from his devices in its motion. But instead, in the Government's view, whether or not the information was disseminated is not material to Plaintiff's claims and is thus not relevant to Defendants' dispositive motion.

CONCLUSION

For the foregoing reasons, Defendants respectfully request that the Court grant their Motion to Dismiss, or in the Alternative, for Summary Judgment.

Dated: October 27, 2011

Respectfully submitted,

TONY WEST
Assistant Attorney General

CARMEN M. ORTIZ
United States Attorney

BARBARA HEALY SMITH
Assistant U.S. Attorney

SANDRA M. SCHRAIBMAN
Assistant Branch Director

s/Diane Kelleher

DIANE KELLEHER
Senior Trial Counsel, U.S. Department of Justice,
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7318
Washington, D.C. 20530
Tel.: (202) 514-4775
Fax.: (202) 616-8470
Email: diane.kelleher@usdoj.gov